UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/679,654 | 10/06/2003 | Keith Bryan Knight | LOT920030023US1 (009) | 4110 |

46321 7590 02/22/2008

CAREY, RODRIGUEZ, GREENBERG & PAUL, LLP
STEVEN M. GREENBERG
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

| EXAMINER | |
|---|---|
| WALSH, JOHN B | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2151 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 02/22/2008 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Application Number: 10/679,654
Filing Date: October 06, 2003
Appellant(s): KNIGHT ET AL.

Steven M. Greenberg
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed December 3, 2007 appealing from the Office action mailed December 21, 2006.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(8) Evidence Relied Upon**

| | | |
|---|---|---|
| 6,081,900 | Subramaniam | 6-2000 |

FTPS, http//en.wikipedia.org/wiki/FTPS, 2 pages, (printed on February 7, 2008).

**(9) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,081,900 to Subramaniam et al.

As concerns claim 1, a method for tunneling (column 11, line 30) non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the method comprising the steps of: soliciting a secured connection with a reverse proxy protecting a back-end server computing

device (figures 1 and 2); establishing a connection with said back-end server computing device via said reverse proxy through said solicitation (figures 1 and 2); and, responsive to establishing said connection, maintaining said connection (figure 2). As concerns the limitation of exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages, Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data (column 7, lines 65-67; col. 9, lines 48-56). One of ordinary skill in the art at the time of the invention would rationalize such a modification since it is a simple substitution of one known element (HTTP) for another (FTP) to obtain predictable results.

As concerns claim 2, the method of claim 1, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy (column 3, line 25).

As concerns claims 3 and 11, wherein said requesting step comprises the steps of: acquiring an address for said reverse proxy and a port for establishing an SSL connection with said reverse proxy (inherent when communicating to acquire an address and port); further acquiring an address for said back-end server computing device and a port for establishing an SSL connection with said back-end server computing device (inherent when communicating to acquire an address and port); formulating an HTTP-CONNECT message using said acquired addresses and ports; and, writing said formulated HTTP-CONNECT message to said reverse proxy (figures 1 and 2).

As concerns claims 4 and 12, wherein said exchanging step comprises the steps of: formatting a buffer with real-time data; and, writing said buffer to said secured connection (column 3, lines 51-52).

As concerns claims 5 and 13, further comprising the step of performing authentication in said reverse proxy as a condition of establishing said secured connection (column 8, lines 40-41).

As concerns claim 6, a system for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the system comprising: a reverse proxy disposed between a client computing device (column 3, line 15) and a server (column 3, lines 14-15) computing device in a computer communications network; an authentication process configured for operation in conjunction with said reverse proxy (figures 1 and 2; column 8, lines 40-41 ); a communications socket established between said reverse proxy and said client computing device (figures 1 and 2); and, a non-HTTP data handler coupled to said secured communications socket and programmed to write non-HTTP data to said reverse proxy without encapsulating said non-HTTP data within HTTP messages (Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data; column 7, lines 65-67 col. 9, lines 48-56).

As concerns claim 7, the system of claim 6, wherein server computing device is a real-time streaming media server, said non-HTTP data handler is a real-time streaming media client, and said non-HTTP data is real-time streaming media (column 5, lines 43-49).

As concerns claim 8, the system of claim 6, wherein said communications socket is a secured sockets layer (SSL) communications link (column 3, line 25).

As concerns claim 9, a machine readable storage having stored thereon a computer program for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the computer program comprising a routine set of instructions for causing the machine to perform the steps of: soliciting a secured connection with a reverse proxy protecting a back-end server computing device (figures 1 and 2); establishing a connection with said back-end server computing device via said reverse proxy through said solicitation (figures 1 and 2); and, responsive to establishing said connection, maintaining said connection (figure 2). As concerns the limitation of exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages, Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data (column 7, lines 65-67 col. 9, lines 48-56).

As concerns claim 10, the machine readable storage of claim 9, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy (column 3, line 25).

**(10) Response to Argument**

*Appellant argues:*

*I. Subramanium does not teach exchanging non-HTTP data over a secured connection without encapsulating the non-HTTP data within HTTP messages.*

*Examiner's response:*

Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data (column 7, lines 65-67). Subramaniam does not disclose that

the FTP data is encapsulated within HTTP data, thus Subramaniam discloses the applicant's claimed limitation of "responsive to establishing said connection, maintaining said connection exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages," since the use of FTP data is non-HTTP data. The applicant has further argued a particular circumstance wherein Subramaniam does not disclose the claimed limitation, however that is one of many circumstances that can be envisioned and the circumstance of using FTP not encapsulated in HTTP messages, is disclosed by Subramaniam (see at least col. 7, lines 65-67 and col. 9, lines 48-56).

*The Appellant argues:*

*II. The Examiner cannot cite Subramanium in support of a rejection under 35 U.S.C. 103(a) based upon what is not taught in Subramanium.*

*The Examiner's response:*

The Appellant argues Subramaniam provides no teaching of any exchange of FTP data outside of the HTTP protocol. See Subramaniam at col. 9, line 48-56 wherein the URL transformer replaces non-secure URLs with secure URLs, wherein the URL may indicate FTP. The URL would indicate FTP not HTTP and is therefore an exchange of FTP data outside of HTTP. The FTP would be transformed into a secure URL which can be FTPS (FTP over SSL) since Subramaniam discloses modifying to promote use of secure sockets layer communication (see col. 3, lines 35-39). (See also *http://en.wikipedia.org/wiki/FTPS* for description of FTP over SSL).

The Appellant further argues the plain text of Subramaniam in column 7 requires the use of HTTP messages for all exchanges of data in the secure connection. The examiner fails to find any explicit disclosure in column 7 or other passages of Subramaniam that recite "the requirement of using HTTP messages for all exchanges of data in the secure connection". Furthermore this statement is contradicted by Subramaniam at least at col. 7, lines 65-67 and col. 9, lines 55-56. Subramaniam provides examples of using the HTTP protocol, however the invention is not drawn to such a narrow scope since the invention is more readily drawn to the transformation of non-secure URLs into secure URLs (col. 10, lines 59-60 "any non-secure data"; col. 13-14, claim 1; col. 2, lines 18-22). Furthermore Figures 1-4 of Subramaniam illustrate their invention without illustrating a specific protocol, such as HTTP data, since the invention does not "require" such a limited scope for operation of the invention Subramaniam. The examiner has given the Appellants claims their broadest reasonable interpretation as well as examining the prior art of Subramaniam in a scope that was disclosed and envisioned by Subramaniam, rather than a narrow perspective as employed by the Appellant in their arguments.

The examiner has not rejected the claims based upon "what is not taught" as alleged by the Appellant. The claims have been given their broadest reasonable interpretation and one of ordinary skill in the art at the time of the invention when presented with Subramaniam (particularly referring to the passages indicated by the Examiner) would conclude that the Appellants claimed invention when given the broadest reasonable interpretation would be taught by Subramaniam.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

John B. Walsh

/John B. Walsh/

Primary Examiner, Art Unit 2151

Conferees:

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2145